Engineering Trustworthy Cryptographic Computations

Yan Huang
Assistant Professor
DES, RSA
Computer Science is no more about computers than astronomy is about telescopes.

Edsger Dijkstra
Cryptography is no more about *hiding messages* than computer science is about computers.
Secure Computation

Good match?
Verifiable Computation

Result correctness?
Homomorphic Encryption

Confidential data?

Proprietary algorithms?
Cryptography Today

- Output
- Correctness
- Program confidentiality
- Inputs
- Privacy
- Output Privacy
Outstanding Challenges

Trustworthy Implementation

Theoretical protocols are \textit{provably secure}, but says nothing about real-world implementations.

Development Cost

- Complex
- Subtle composition
- Interactive

\[
c \leftarrow \text{Enc}(k, m)
\]

\[
f' \leftarrow \pi (k, f)
\]
Outstanding Challenges

Trustworthy Implementation
Theoretical protocols are provably secure, but says nothing about real-world implementations.

Development Cost
- Complex
- Subtle composition
- Interactive

Higher-order Functions

\[ f' \leftarrow \pi (k, f) \]
A Functional Solution for Trustworthiness

Untrusted but automatically verifiable implementation

Real Implementation

An chain of changes along with short proofs

Ideal functionality

Hardness assumptions

Proof verifier

Small Trusted Base
A Functional Approach

Gemone Matching
Machine Learning
Intrusion Detection

Application

Computational Model

Homomorphic Enc.
Verifiable Computation
Secure Computation
Ind. Obfuscation

Cryptography
Your Killer Application Ideas?